



Nortel Secure Network Access

Installation — Quick Start Switch 4070

Nortel Secure Network Access
Document status: Standard
Document version: 01.01
Document date: 28 July 2008

Copyright © 2008, Nortel Networks
All Rights Reserved.

Sourced in Canada, the United States of America, and India

LEGAL NOTICE

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS "WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

Contents

Regulatory Information and Safety Precautions	5
International Regulatory Statements of Conformity	5
National Electromagnetic Compliance (EMC) Statements of Compliance	5
FCC statement (USA only)	5
ICES statement (Canada only)	6
Canadian Department of Communications Radio Interference Regulations	6
Règlement sur le brouillage radioélectrique du ministère des Communications	6
CE marking statement (Europe only)	6
EN 55022 statement	6
EN 55024 statement	6
European Union and European Free Trade Association (EFTA) notice	6
VCCI statement (Japan/Nippon only)	7
MIC notice (Republic of Korea only)	7
National Safety Statements of Compliance	7
EN 60950 statement	7
NOM statement (Mexico only)	7
Información NOM (unicamente para México)	8
Denan statement (Japan/Nippon only)	8
National Environmental Statements of Compliance	9
Restriction on Hazardous Substances Directive Compliance Statement	9
WEEE Directive Compliance Statement	9
Notices	9
Cautions and Warnings	10
Software license	13
New in this release	17
Features	17
Other changes	17
Introduction	19
Prerequisites	19
Navigation	19
Installation preparation	21
Navigation	21

Safety precautions	21
Safety precautions navigation	21
Installation checklist	23
Installation	25
Navigation	25
Unpacking the device	25
Installing an NSNA device into a rack	26
Prerequisites for installing an NSNA into a rack	26
Cabling the device	30
Cabling the device navigation	30
Connecting network cables	30
Connecting serial cables	30
Configuration	33
Navigation	33
Creating a new cluster	33
Prerequisites	33
Joining an SNAS to an existing cluster	36
Enabling the browser-based interface	38
Applying the Nortel SNAS license	40

Regulatory Information and Safety Precautions

Read the information in this section to learn about regulatory conformities and compliances.

International Regulatory Statements of Conformity

This is to certify that the Nortel Secure Network Access Switch equipment was evaluated to the international regulatory standards for electromagnetic compliance (EMC) and safety and were found to have met the requirements for the following international standards:

- EMC – Electromagnetic Emissions – CISPR 22, Class A
- EMC – Electromagnetic Immunity – CISPR 24
- Electrical Safety – IEC 60950, with CB member national deviations

Further, the equipment has been certified as compliant with the national standards as detailed below.

National Electromagnetic Compliance (EMC) Statements of Compliance

FCC statement (USA only)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission (FCC) rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures may be necessary to correct the interference at their own expense.

ICES statement (Canada only)

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (Nortel Secure Network Access Switch) does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (le commutateur Nortel Secure Network Access Switch) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

CE marking statement (Europe only)

EN 55022 statement

This is to certify that the Nortel Secure Network Access Switch equipment is shielded against the generation of radio interference in accordance with the application of Council Directive 2004/108/EC. Conformity is declared by the application of EN 55022 Class A (CISPR 22).



CAUTION

This device is a Class A product. In a domestic environment, this device can cause radio interference, in which case the user may be required to take appropriate measures.

EN 55024 statement

This is to certify that the Nortel Secure Network Access Switch is shielded against the susceptibility to radio interference in accordance with the application of Council Directive 2004/108/EC. Conformity is declared by the application of EN 55024 (CISPR 24).

European Union and European Free Trade Association (EFTA) notice



All products labeled with the CE marking comply with R&TTE Directive (1995/5/EEC) which includes the Electromagnetic Compliance (EMC) Directive (2004/108/EC) and the Low Voltage Directive (2006/95/EC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms (ENs). The equivalent international standards are listed in parenthesis.

- EN 55022 (CISPR 22)—Electromagnetic Interference

- EN 55024 (IEC 61000-4-2, -3, -4, -5, -6, -8, -11)—Electromagnetic Immunity
- EN 61000-3-2 (IEC 610000-3-2)—Power Line Harmonics
- EN 61000-3-3 (IEC 610000-3-3)—Power Line Flicker

VCCI statement (Japan/Nippon only)

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI) for information technology equipment. If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

MIC notice (Republic of Korea only)

This device has been approved for use in Business applications only per the Class A requirements of the Republic of Korea Ministry of Information and Communications (MIC). This device may not be sold for use in a non-business application.

Observe the Regulatory Marking label on the back or bottom of each switch for specific certification information pertaining to this model. Each Nortel Secure Network Access Switch model is approved for shipment to/usage in Korea and is labeled as such, with all appropriate text and the appropriate MIC reference number.

National Safety Statements of Compliance

EN 60950 statement

This is to certify that the Nortel Secure Network Access Switch equipment is in compliance with the requirements of EN 60950 in accordance with the Low Voltage Directive. Additional national differences for all European Union countries have been evaluated for compliance.

NOM statement (Mexico only)

The following information is provided on the devices described in this document in compliance with the safety requirements of the Norma Oficial Mexicana (NOM):

Exporter:	Nortel Networks, 4655 Great America Parkway, Santa Clara, CA 95054 USA.
Importer:	Nortel Networks de México, S.A. de C.V. Avenida Insurgentes Sur #1605 Piso 30, Oficina Col. San Jose Insurgentes Deleg-Benito Juarez México D.F. 03900
Tel:	52 5 480 2100
Fax:	52 5 480 2199
Input:	Model SNAS 4070 AC Redundant Power Supply – 835W Input: 100-127 VAC 10.0A, 200-240 VAC 5A 50-60 HZ

Información NOM (unicamente para México)

La información siguiente se proporciona en el dispositivo o en los dispositivos descritos en este documento, en cumplimiento con los requisitos de la Norma Oficial Mexicana (NOM):

Exportador:	Nortel Networks, 4655 Great America Parkway, Santa Clara, CA 95054 USA.
Importer:	Nortel Networks de México, S.A. de C.V. Avenida Insurgentes Sur #1605 Piso 30, Oficina Col. San Jose Insurgentes Deleg-Benito Juarez México D.F. 03900
Tel:	52 5 480 2100
Fax:	52 5 480 2199
Embarcar a:	Modele SNAS 4070 AC Redundant Power Supply – 835W Input: 100-127 VAC 10.0A, 200-240 VAC 5A 50-60 HZ

Denan statement (Japan/Nippon only)

本製品を安全にご使用頂くため、以下のことにご注意ください。

- 接続ケーブル、電源コード、ACアダプタなどの部品は、必ず製品に同梱されております添付品または指定品をご使用ください。添付品・指定品以外の部品をご使用になると故障や動作不良、火災の原因となることがあります。
- 同梱されております付属の電源コードを他の機器には使用しないでください。上記注意事項を守らないと、死亡や大怪我など人身事故の原因となることがあります。

National Environmental Statements of Compliance

The WEEE Directive 2002/96/EC and RoHS (Restriction of Hazardous Substances) Directive 2002/95/EC sets collection, recycling and recovery targets for various categories of electrical products and their waste.

Restriction on Hazardous Substances Directive Compliance Statement

The Restriction on Hazardous Substances Directive (RoHS) (2002/95/EC), which accompanies the WEEE Directive, bans the use of heavy metals and brominated flame-retardants in the manufacture of electrical and electronic equipment. Specifically, restricted materials under the RoHS Directive are Lead (including solder used in PCB's), Cadmium, Mercury, Hexavalent Chromium, and Bromine.

Nortel declares compliance with the European Union (EU) RoHS Directive (2002/95/EC).

WEEE Directive Compliance Statement



This product at end of life is subject to separate collection and treatment in the EU Member States, Norway, and Switzerland and therefore is marked with the symbol shown at the left. Treatment applied at end of life of these products in these countries shall comply with the applicable national laws implementing Directive 2002/96/EC on Waste of Electrical and Electronic Equipment (WEEE).

Nortel declares compliance with the European Union (EU) WEEE Directive (2002/96/EC).

Notices

Notice paragraphs alert you about issues that require your attention. The following paragraphs describe the types of notices used in this guide.



CAUTION ESD

ESD notices provide information about how to avoid discharge of static electricity and subsequent damage to Nortel products.



CAUTION

Caution notices provide information about how to avoid possible service disruption or damage to Nortel products.



WARNING

Warning notices provide information about how to avoid personal injury when working with Nortel products.



DANGER

Danger — High Voltage notices provide information about how to avoid a situation or condition that can cause serious personal injury or death from high voltage or electric shock.



DANGER

Danger notices provide information about how to avoid a situation or condition that can cause serious personal injury or death.

Cautions and Warnings



WARNING

Installation must be performed by qualified service personnel only. Read and follow all warning notices and instructions marked on the product or included in the documentation.



WARNING

This product relies on the building's installation for overcurrent protection. Ensure that a fuse or circuit breaker no larger than 120 VAC, 15A U.S. (240 VAC, 10 A international) is used on the phase conductors.

**CAUTION**

To reduce the risk of fire, use only number 26 AWG or larger UL Listed or CSA Certified Telecommunication Line Cord for all network connections.

**WARNING**

Before working on this equipment be aware of good safety practices and the hazards involved with electrical circuits.

Trademarks

*Nortel, Nortel Networks, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

Adobe and Adobe Reader are trademarks of Adobe Systems Incorporated.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation.

The asterisk after a name denotes a trademarked item.

Software license

This section contains the Nortel Networks software license.

Nortel Networks software license agreement

This Software License Agreement ("License Agreement") is between you, the end-user ("Customer") and Nortel Networks Corporation and its subsidiaries and affiliates ("Nortel Networks"). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

"Software" is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. **Licensed Use of Software.** Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment ("CFE"), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except

as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer's Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. **Warranty.** Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided "AS IS" without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.
3. **Limitation of Remedies.** IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The foregoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.
4. **General**
 - a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software

documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

- b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.
- c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.
- d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.
- e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.
- f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

New in this release

The following sections detail what's new in *Nortel Secure Network Access Installation — Quick Start Switch 4070* (NN47230-303) for Release 2.0.

- ["Features" \(page 17\)](#)
- ["Other changes" \(page 17\)](#)

Features

This is the first standard release of the document.

Other changes

None.

Introduction

The Nortel Secure Network Access Switch (NSNA) 4070 Quick Start Guide provides basic instructions about installing the hardware and performing basic configuration and management of the network.

The Nortel Secure Network Access Solution (Nortel SNAS) is a clientless solution that provides seamless, secure access to the corporate network from inside or outside the network. This contributes to the quality of the end user experience by allowing web-based applications to operate more efficiently.

Prerequisites

This guide is intended for network installers and system administrators engaged in the configuration and management of a network. This guide assumes a familiarity with the following topics:

- networks, Ethernet bridging, and IP routing
- networking concepts and terminology
- windowing systems and graphical user interfaces (GUI)
- network topologies

Navigation

- ["Installation preparation" \(page 21\)](#)
- ["Installation" \(page 25\)](#)
- ["Configuration" \(page 33\)](#)

Installation preparation

This section provides basic information about the Nortel Secure Network Access Switch (NSNA) 4070 and the checklist of the shipped accessories.

Navigation

- ["Safety precautions" \(page 21\)](#)
- ["Installation checklist" \(page 23\)](#)

Safety precautions

This section describes the safety precautions, which are vital for handling and installation of the NSNA.

Safety precautions navigation

- ["Personal safety before installing the device" \(page 21\)](#)
- ["Module safety" \(page 21\)](#)
- ["Cable and connector safety" \(page 22\)](#)

Personal safety before installing the device

For your safety, review the following personal safety warnings before working with the NSNA.

- Two or more people must be involved in installing the device.
- Use the following safe practices for lifting:
 - Items between 18 and 32 kilograms (39.7 and 70.5 pounds) should be lifted by a minimum of two people.

Module safety

Use the following general practices to prevent the equipment damage when working with the NSNA.

- The device must be installed in a room where the ambient temperature is at or below 35 degrees Celsius (95 degrees Fahrenheit).

- To promote proper air circulation, ensure the device vents are not blocked or obstructed by cables, panels, server rack frames, or other materials. A minimum of 15 centimeters (6 inches) of space provides proper airflow.
- To prevent damage to server components, always install a blank filler panel to cover the open space and ensure proper air circulation.
- Install the device only in a server rack with perforated doors.
- Plan the device installation starting from the bottom of the server rack.
- Install the heaviest device in the bottom of the server rack.
- Do not extend more than one device out of the server rack at the same time.
- Remove the server rack doors and side panels to provide easier access during installation.
- Connect the device to a properly grounded outlet.
- Do not overload the power outlet when multiple devices are installed in the server rack.
- Install the device in a server rack that meets the following requirements:
 - Minimum depth of 70 millimeters (2.76 inches) between the front mounting flange and inside of the front door.
 - Minimum depth of 157 millimeters (6.18 inches) between the rear mounting flange and inside of the rear door.
 - Minimum depth of 718 millimeters (28.27 inches) and maximum depth of 762 millimeters (30 inches) between the front and rear mounting flanges to support the use of the cable-management arm.
- Do not place any object directly on a server rack mounted device. Server rack mounted devices are not meant to be load bearing units.
- When mounting this device in a server rack, do not stack units directly on top of one another in the rack. Each unit must be secured with appropriate mounting brackets. Mounting brackets are not designed to support multiple units.

Cable and connector safety

Use the following instructions to safeguard cables and connectors while working with the NSNA.

- Connect the device to a properly grounded outlet.
- Do not overload the power outlet when multiple devices are installed in the server rack.

Installation checklist

This checklist represents the high-level tasks that must be performed to successfully install the Nortel Secure Network Access Switch. Device installation involves the following steps:

Procedure steps

Step	Action
1	<p>Choose a suitable location to install the device.</p> <p>Use the information contained in the following sections to determine where the device should be installed:</p> <ul style="list-style-type: none">• Safety and installation precautions• Hardware specifications
2	<p>Unpack the device from the shipping container.</p> <p>Unpack all items from the original packaging and determine if all items have been shipped. All items listed in Package contents should be present. If items are missing, contact the party from whom the Nortel Secure Network Access Switch was purchased.</p>
3	<p>Mount the switch.</p> <p>To rack mount the Nortel Secure Network Access Switch, see the Installing the Nortel SNAS 4070 in Nortel Secure Network Access Installation — Switch, NN47230-302.</p> <p>The Nortel Secure Network Access Switch is intended to be installed in a 4 post server rack. The device cannot be installed in a 2 post equipment rack. It needs to be installed in a server rack, which is a 4 post rack.</p>
4	<p>Connect the device power units to an appropriate, properly grounded power source.</p>
5	<p>Connect network cables to the device.</p>
6	<p>Power on the switch by depressing the power button on the front of the unit.</p>

—End—

Installation

This chapter contains installation instructions for the Nortel Secure Network Access Switch (NSNA).

Navigation

- "Unpacking the device" (page 25)
- "Installing an NSNA device into a rack" (page 26)
- "Cabling the device" (page 30)

Unpacking the device

Unpack the shipping container to ensure the device and all accessories are included and undamaged.

Procedure steps

Step	Action
------	--------

- 1 Remove the equipment from the shipping container and place the device on antistatic material.
- 2 Check all items for damage.

ATTENTION

If the equipment is damaged, contact your Nortel sales representative.

- 3 Use the following device shipping accessories checklist to verify that in the shipping container includes all contents.

Check	Accessory	Use to
	Switch	Install in a 4 post server rack.
	Power units	Connect the units to an appropriate and properly grounded power source.
	Network cables	Connect the device.

Check	Accessory	Use to
	copper network interface card	Connect the network cables.
	Console cable	Establish a console connection to the device.

—End—

Installing an NSNA device into a rack

Install an NSNA in a standard equipment rack.

Prerequisites for installing an NSNA into a rack

- Do not install the device in the network equipment racks

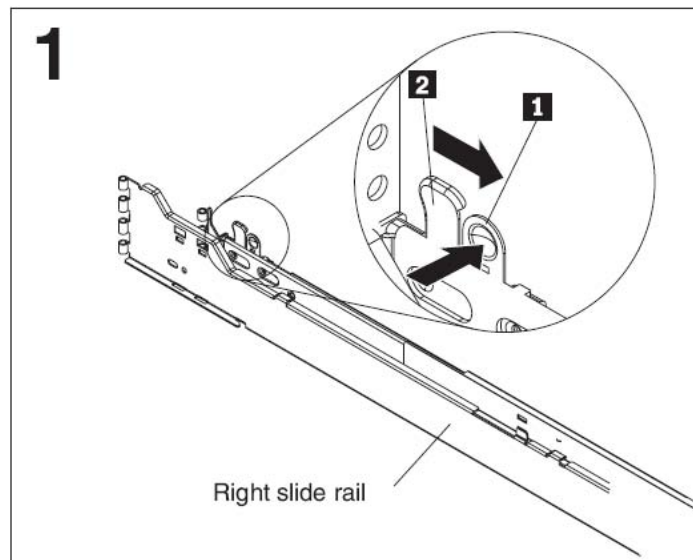
The following procedure describes how to rack-mount the device. Observe all safety and precautionary warnings in this procedure. Review Safety and installation precautions before proceeding with the installation process.

To install the Nortel Secure Network Access Switch, perform the following tasks. Throughout the following procedure, bold numbers in brackets are presented. These correspond with the numbers in the step illustration to provide a visual reference for the installation procedure steps.

Procedure steps

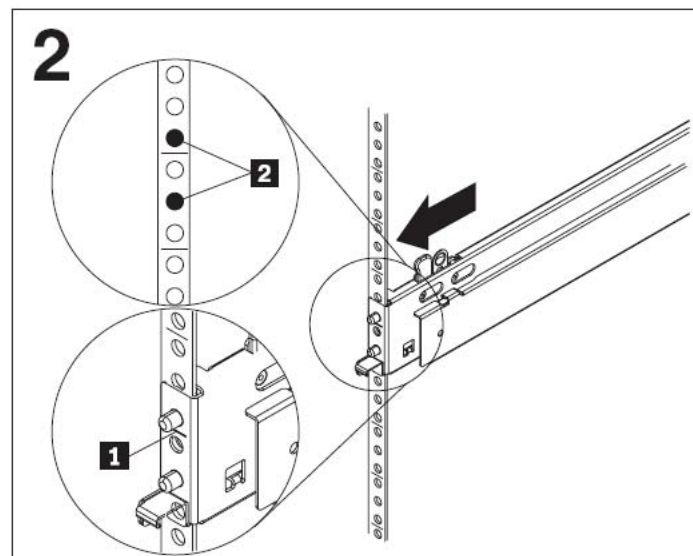
Step	Action
------	--------

- | | |
|---|---|
| 1 | Hold the left and right slide rails and separate them from the other device hardware. Take one slide rail and push outward on the slide rail latch (1) and pull the latch back to open the slide rail (2). The latch catches to stay open. Repeat the procedure for the other end of the slide rail and then again for the other slide rail provided. |
|---|---|



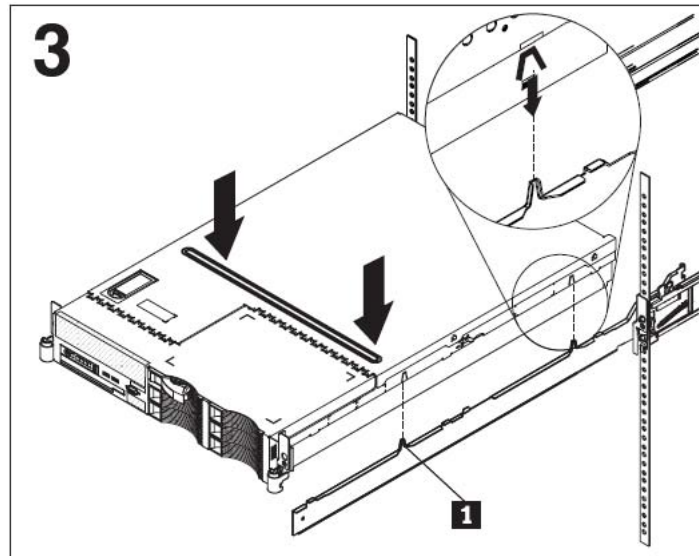
- 2 Align the slide rail with the front mounting flange by aligning the score mark on the slide rail (1) with the score mark on the rail between the upper and lower U. Push outward on the slide rail latch to close to the latch and secure the slide rail. Do the same for the other front of the slide rail. Align the slide rail with the rear mounting flange and close the latches for the rear of the slide rail to secure it.

Ensure the slide rails are securely seated on the mounting flanges. When the slide rails are secure, the slide rail pins protrude from the slide rails (2).



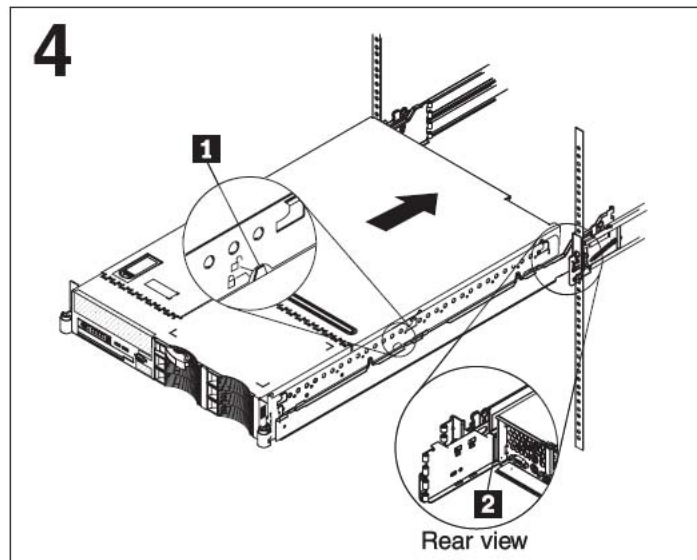
- 3 Extend the slide rails fully from the server rack until they lock. Align the tabs on the slide rails with the matching inserts on the device (1) and lower the server onto the slide rails.

Ensure that each slide rail tab is inserted in the matching insert on the server and that the server is resting on the top edge of the slide rail.

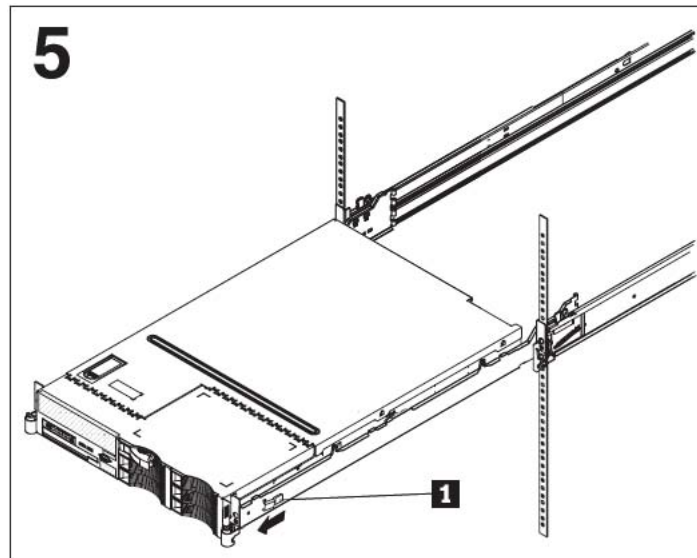


- 4 Carefully slide the device along the slide rails approximately 2.54 centimeters (1 inch) toward the server rack to lock the device on the slide rails. When the device is locked in position, an indicator (1) is visible on each side of the device. Ensure that the device is securely attached to the slide rail hooks (2).

To remove the device from the rack, lift up on the indicator and slide the server forward.

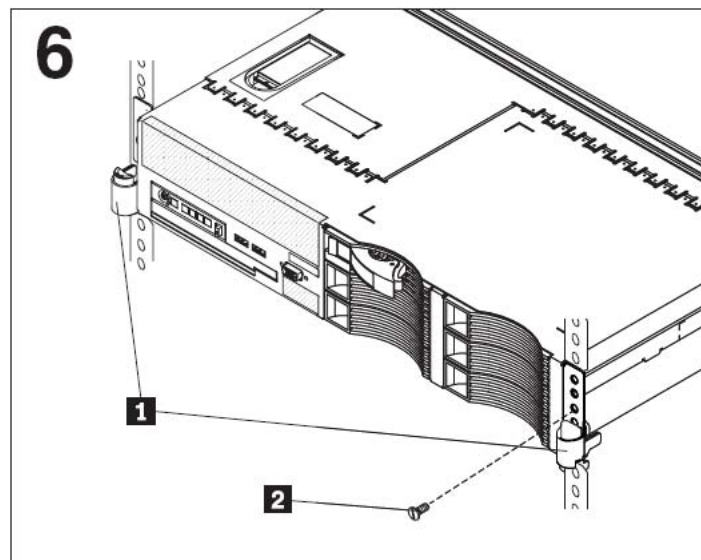


- 5 Lift the locking levers (1) on the slide rails and slide the device into the server rack until it extends approximately 10.16 centimeters (4 inches) from the rack.



- 6 Slide the device into the server rack cabinet until the release latches (1) lock into place. To slide the device out of the rack, press on the release latches.

Insert the included, optional M6 screws in the front and rear of the device (2) if moving the server rack or the rack is installed in a vibration prone area.



—End—

ATTENTION

To remove the device, reverse these instructions.

Cabling the device

This section describes about cabling the device for network and console connections.

Cabling the device navigation

- ["Connecting network cables" \(page 30\)](#)
- ["Connecting serial cables" \(page 30\)](#)

Connecting network cables

The Nortel Secure Network Access Switch 4070 contains copper network interface card running at Intel Dual LAN 10/100/1000.

Connecting serial cables

This section describes how to connect a DB9 serial cable to establish a console connection to the device.

Procedure steps

Step Action

- 1 Prepare either an ASCII terminal or a computer running terminal emulation software to serve as the command device.
- 2 Configure the terminal or computer with the following parameters:

Serial connection parameters

Parameter	Value
Baud Rate	9600
Data Bits	8
Parity	None
Stop Bits	1
Flow Control	None

- 3 Connect one end of the serial cable to the terminal or computer.
- 4 Connect the other end of the serial cable to the serial connector located at the rear of the device.
- 5 Proceed with establishing the console connection.

—End—

Configuration

This chapter contains configuration instructions for commissioning the Nortel Secure Network Access Switch.

Navigation

- ["Creating a new cluster" \(page 33\)](#)
- ["Joining an SNAS to an existing cluster" \(page 36\)](#)
- ["Enabling the browser-based interface" \(page 38\)](#)
- ["Applying the Nortel SNAS license" \(page 40\)](#)

Creating a new cluster

This section describes how to create a new cluster.

Nortel Secure Network Access Switch (Nortel SNAS) is member of a cluster. A cluster can consist of a single unit or a group of units that share the same configuration parameters. There can be more than one cluster in the network, each with its own set of parameters and services.

Establish a console connection by cabling the unit to a terminal or a computer running a terminal emulator session.

Prerequisites

- Establish a console connection by cabling the unit to a terminal or a computer running a terminal emulator session.

Procedure steps

Step	Action
1	Using the supplied console cable, connect the terminal to the console port.
2	Power on the terminal and the Nortel Secure Network Access Switch 4070.

- 3 To initiate the system connection process, press ENTER on the terminal.
- 4 At the login prompt, log in as user: admin.
- 5 At the password prompt, enter the administrator password. The default administrator password is admin.

ATTENTION

To ensure continuing system security, change the default password to the password of your choice after you successfully configure the switch.

- 6 After password verification, when the device is booted for the first time, the **Setup** menu is displayed. Use the **new** command to begin cluster creation.

```
[Setup Menu]
join - Join an existing iSD cluster
new - Initialize host as a new installation
boot - Boot menu
info - Information menu
exit - Exit [global command, always available]
>> Setup# new
Setup will guide you through the initial configuration.
```

- 7 Specify the network connectivity port.

```
Enter port number for the management interface [1-3]:
```

ATTENTION

The Nortel SNAS 4070 has two ports for the management interface.

This port is assigned to Interface 1.

- 8 Specify the host IP address.

```
Enter IP address for this machine (on management
interface):
```

The IP address must be unique and within the same address range as the Management IP address. The host IP address is assigned to Interface 1.

- 9 Enter network mask.

```
Enter network mask [255.255.255.0]:
```

Specify the desired network mask or accept the suggested value by pressing ENTER. If a connected router or switch attaches VLAN tag IDs to incoming packets, specify the VLAN tag ID used.

- 10 Setup a two armed configuration.

```
Setup a two armed configuration (yes/no):
```

- 11 Enter a default gateway address.

```
Enter default gateway IP address (or blank to skip):
```

Enter a default gateway IP address that is within the same network address range as the host IP address.

- 12 Enter a Management IP address (MIP).

```
Enter the Management IP (MIP) address:
Making sure the MIP does not exist...ok
Trying to contact gateway...ok
```

Enter a unique Management IP address (MIP) that is within the same network address range as the host IP address and the default gateway IP address.

- 13 Configure the time zone, NTP, and DNS server settings.

Configuration of NTP is optional and can be accomplished later.

```
Enter a timezone or 'select' [select]:
Select a continent or ocean:
Select a country:
Select a region:
Selected timezone:
Enter the current date (YYYY-MM-DD) [2006-03-01]:
Enter the current time (HH:MM:SS) [09:26:16]:
Enter NTP server address (or blank to skip):
Enter DNS server address:
```

- 14 Generate new SSH host keys and define a password for the **admin** user.

```
Generate new SSH host keys (yes/no) [yes]:
This may take a few seconds...ok
Enter a password for the "admin" user:
Re-enter to confirm:
```

To maintain a high level of security while using an SSH connection, accept the default choice to generate new SSH host keys.

- 15 If you like to go through setup.

```
Run NSNAS quick setup wizard [yes/no] [yes]
```

- 16 Cluster creation is complete. Login using the `admin` user to continue with configuration.

—End—

Joining an SNAS to an existing cluster

This section describes how to set up one-armed configuration to add additional NSNA to an existing cluster by specifying the Management IP address (MIP).

While joining SNAS to an existing cluster, less information is needed because the new SNAS fetches most of the configuration from the other SNAS(s) in the cluster.

Prerequisites

- For the cluster configuration, all the nodes must be on a same subnet.
- If the Access list consists of entries (e.g. IP addresses for control of Telnet and SSH access), add the cluster's MIP, the existing SNAS host IP address on Interface 1, and the host IP address for the new SNAS to the Access list. This must be done before you join the new SNAS, or the devices cannot communicate. Use `/cfg/sys/accesslist` to check the Access list. If the Access list is empty, this step is not required.
- If the SNAS you are about to join contains a different software version than existing SNAS(s), install the preferred software version on the new SNAS before you join it or upgrade the whole cluster to the same software version as the new SNAS. Use `/boot/software/cur` to check the currently installed software version.

Procedure steps

Step	Action
------	--------

- 1 Choose **join** from the Setup menu to add an SNAS to an existing cluster.

```

-----
[Setup Menu]
  join      - Join an existing cluster
  new       - Initialize host as a new installation
  boot      - Boot menu
  info      - Information menu
  exit      - Exit [global command, always available]

>> Setup# join
Application Optimizer Setup will guide you through the initial configuration.

```

- 2 Specify the port to be used for network connectivity.

```
Enter port number for the management interface [1-3]:
```

This port is automatically assigned to Interface 1. This interface can be used for both management traffic (coming from the private intranet) and client traffic (coming from the public Internet).

If port 1 is the management interface port for existing SNAS(s), Nortel recommends that you configure port 1 for the new SNAS as well.

- 3 Enter the new SNAS host IP address.

```
Enter IP address for this machine (on management interface): <ip address>
```

This IP address should be within the same network address range as the cluster's Management IP address.

- 4 Enter the network mask.

```
Enter network mask [255.255.255.0]: 255.255.255.0
```

Specify the desired network mask or press **Enter** to accept the suggested value. If a connected router or switch attaches VLAN tag IDs to incoming packets, specify the VLAN tag ID to use.

- 5 Press **Enter** to create a one-armed configuration.

```
The system is initialized by connecting to the management server
on an existing cluster, which must be operational and initialized.
```

- 6 Enter the Management IP address (MIP) of the existing cluster.

```
Enter the Management IP (MIP) address: 10.9.254.55
```

Provide the Management IP address of the cluster to which you want to join the new SNAS. To check the Management IP of an existing cluster, connect to the cluster and use the `/cfg/sys/cur` command.

- 7 Provide the correct `admin` user password.

```
Enter the existing admin user password:
```

—End—

The SNAS that is joined to the cluster automatically picks up all configuration data from an installed SNAS in the cluster.

Wait until the Setup utility gets finished.

The login prompt appears.

```
login: admin
Password:
```

Log in as `admin` to continue to configure the SNAS cluster using the CLI or the BBI.

Enabling the browser-based interface

The SNAS browser-based interface (BBI) is not immediately available for use when the device is first commissioned. The BBI can be enabled to work over HTTP, HTTPS, or both protocols. It is recommended the default ports of 80 (HTTP) and 4443 (HTTPS) be changed when it comes to device management. HTTP and HTTPS client traffic is connected through these default ports and if used in device management cannot be available to service requests.

To enable the BBI, perform the following procedure:

Procedure steps

Step	Action
1	Establish a console connection or Telnet session with the device.
2	Log into the switch with an administrative user name and password.
3	From the main Command Line Interface (CLI) prompt, enter the Administrative Applications menu with the <code>/cfg/sys/adm</code> command.
	<pre>>> Main# /cfg/sys/adm</pre>
4	From the Administrative Applications menu prompt, use the <code>http</code> command to enter HTTP access menu.
	<pre>>> Administrative Applications# http</pre>
5	From the HTTP access menu, designate a port for HTTP access using the <code>port</code> command.
	<pre>>> HTTP# port <port_number></pre>
	Using a port other than 80 requires the user to designate the port when accessing the BBI. For example, if the device IP address is 192.168.0.3 and the designated port is 8080, the device is accessed from the browser as: http://192.168.0.3:8080 .
6	From the HTTP access menu, enable BBI access using the <code>ena</code> command.
	<pre>>> HTTP# ena</pre>
7	Finalize the changes using the <code>apply</code> command.
	<pre>>> HTTP# apply</pre>
	Steps 8 through 11 provide instruction on enabling HTTPS access to the BBI. Enabling HTTPS is not necessary for access to the BBI but provides a more secure environment than HTTP access.
8	(Optional) From the Administrative Applications menu prompt, use the <code>https</code> command to enter HTTPS access menu.

```
>> Administrative Applications# https
```

- 9 (Optional) From the HTTPS access menu, designate a port for HTTPS access using the **port** command.

```
>> HTTPS# port <port_number>
```

Using a port other than 4443 requires the user to designate the port when accessing the BBI. For example, if the device IP address is 192.168.0.3 and the designated port is 465, the device is accessed from the browser as: **https://192.168.0.3:465**.

- 10 (Optional) From the HTTPS access menu, enable BBI access using the **ena** command.

```
>> HTTPS# ena
```

- 11 (Optional) Finalize the changes using the **apply** command.

```
>> HTTPS# apply
```

—End—

Applying the Nortel SNAS license

The Nortel SNAS ships with support for up to 200 authenticated user sessions. To support additional users on your Nortel SNAS switch, you must obtain a Nortel SNA software license file. The software license file contains a software license key that you must enter into the Nortel SNAS switch to activate support for the additional users. The file can support an additional 100, 250, 500, 1000, 2000, or, 5000 users.

The following table lists the part number for the additional concurrent endpoints.

Part Number	Description
EB1639171	Secure Network Access License - Add 100 concurrent endpoints
EB1639172	Secure Network Access License - Add 250 concurrent endpoints
EB1639175	Secure Network Access License - Add 500 concurrent endpoints
EB1639182	Secure Network Access License - Add 1000 concurrent endpoints

Part Number	Description
EB1639183	Secure Network Access License - Add 2000 concurrent endpoints
EB1639184	Secure Network Access License - Add 5000 concurrent endpoints

Procedure steps

Step	Action
------	--------

- | | |
|---|--|
| 1 | Contact Nortel Customer Support and purchase part number.
In North America, Nortel Customer Support can be contacted at 1-800-4NORTEL (1-800-466-7835). For phone numbers outside of North America, refer to http://www.nortel.com/callus . |
| 2 | Once this is purchased, Nortel Customer Support sends a certificate that contains a unique product code and an e-mail address. Send this unique product code and the device MAC address to the e-mail address provided. The device MAC address can be obtained by using the <code>/info/local</code> command in the CLI. |

```
>> Main# /info/local
```

- | | |
|---|---|
| 3 | After the unique product code and device MAC address is verified, a keycode is sent back to you. Use this keycode to enable additional authenticated user sessions. |
|---|---|

—End—

The keycode is applied to the device through either the CLI or the BBI. Perform one of the following procedures to apply the license keycode.

Through BBI

Procedure steps

Step	Action
------	--------

- | | |
|---|---|
| 1 | Click Config . |
| 2 | Select Cluster > Host > License from the BBI menu. |
| 3 | Paste the keycode in the text box labeled New License . |
| 4 | Click Save . |

—End—

Through CLI

Procedure steps

- | Step | Action |
|------|---|
| 1 | Enter the command <code>/cfg/sys/host <host_number>/license</code> . |
| 2 | Enter the keycode. |
| 3 | Press Enter on the keyboard to create a new line and type three periods (...). |
| 4 | Press Enter to input the keycode. |
| 5 | Use the apply command to save the license and enable the feature. |

```
>> Main# /cfg/sys/host <host_number>/license
```

```
>> Cluster Host 1# apply
```

The SNAS is now enabled to support additional authenticated user sessions.

—End—

Nortel Secure Network Access

Installation — Quick Start Switch 4070

Copyright © 2008, Nortel Networks
All Rights Reserved.

Publication: NN47230-303
Document status: Standard
Document version: 01.01
Document date: 28 July 2008

To provide feedback or report a problem in this document, go to <http://www.nortel.com/documentfeedback>.

Sourced in Canada, the United States of America, and India

LEGAL NOTICE

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Nortel, the Nortel logo, and the Globemark are trademarks of Nortel Networks.

All other trademarks are the property of their respective owners.

